PERKINSCOIE

1888 Century Park East
Suite 1700
Los Angeles, CA 90067-1721

T +1.310.788.9900
F +1.310.788.3399
PerkinsCoie.com

March 10, 2021

Dominique Regine Shelton Leipzig
DSheltonLeipzig@perkinscoie.com
D. +1.310.788.3327
F. +1.310.843.1245
Arsen Kourinian
AKourinian@perkinscoie.com
D. +1.310.788.3233
F. +1.310.843.2805

VIA E-MAIL & U.S. 1ST-CLASS MAIL

Washington State
Office of the Attorney General
1125 Washington St. SE
P.O. Box 40100
Olympia, WA 98504
Email: SecurityBreach@atg.wa.gov

Re: Notification of Data Security Incident

Dear Attorney General Ferguson:

We represent Mead Johnson & Company, LLC ("MJN") with respect to a recent data security incident involving Personal Information (as defined under Wash. Rev. Code § 19.255.005) held by MJN's vendor, ActiveProspect, Inc. ("ActiveProspect"). ActiveProspect is a vendor retained by MJN that conducts quality control of consumer leads. The leads contain data provided by consumers interested in products offered by MJN. The data security incident involving data held by ActiveProspect is described in greater detail below. MJN takes the protection of Personal Information very seriously and is taking steps to remediate this issue. This notice may be supplemented if any new significant facts are learned subsequent to its submission.

1. Nature of the Security Incident and Number of Washington Residents Affected.

On or around November 7 and 8, 2020, an unknown outside actor using the user credentials of an employee of ActiveProspect gained access to MJN's account data. ActiveProspect learned of the security incident on November 20, 2020, while conducting a routine audit. ActiveProspect provided its initial notice to MJN regarding this security incident on December 2, 2020. However, the full scope and extent of the Personal Information that may have been accessed by the threat actor was not known to MJN until it had an opportunity to conduct an investigation on or around February 23, 2021. On or about that date, MJN, working with its investigator, learned that the account file maintained by ActiveProspect contained the Personal Information of 2,828 Washington residents, including first and last name, in combination with date of birth.

2. Steps Taken in Response to the Data Security Incident.

From our understanding, this was the first time that our vendor, ActiveProspect, experienced a data breach. After learning of the incident on November 20, 2020, ActiveProspect has indicated to MJN that it has taken remediation steps, including deleting the ActiveProspect employee's

account, deleting the fraudulent accounts believed to have been created by the threat actor, working with its employees to reset passwords, providing further training to its employees regarding the company's security policy, and instituting further administrative and technical safeguards. ActiveProspect has hired a cybersecurity firm, which has monitored the dark web for any of the affected data. It has confirmed that none of the affected residents' information has materialized in the dark web. The firm continues to monitor for any potential exposure of the information online and ActiveProspect will notify MJN immediately of identified misuse. In addition, while MJN is currently not aware of any misuse of the Personal Information compromised during this incident, MJN is providing twelve (12) months of credit and identity monitoring services to each letter recipient at no cost through Experian.

3. Contact Information.

MJN remains dedicated to data privacy and security. If you have any questions or need additional information, please do not hesitate to contact me at (310) 788-3327 or by e-mail at DSheltonLeipzig@perkinscoie.com.

Very truly yours,

Dominique Shelton Leipzig

Encl.: Consumer Notification Letter

Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

March 10, 2021

G3025-L02-0000002 T00001 P001 *****AUTO**MIXED AADC 159
SAMPLE A. SAMPLE - L02-WA
APT ABC
123 ANY ST
ANYTOWN, ST 12345-6789

Dear Sample A. Sample:

In the interest of transparency, Mead Johnson & Company, LLC ("Mead Johnson") is notifying you that one of our vendors, ActiveProspect, discovered an incident that may affect the security of some of your protected personal information, which pursuant to Washington law is limited only to your first name, last name and date of birth. As detailed below, an unauthorized party gained access to a file containing your personal information, noted above. Mead Johnson has not seen any of your personal information being placed or sold online. ActiveProspect continues to monitor for any risk of exposure. Therefore, Mead Johnson has no reason to believe that you are at risk of harm. Nonetheless, should this incident give you any concern, we have arranged for you to receive one year of complimentary credit and identity monitoring through Experian (details for signing up below).

1. What Happened?

On November 7 and 8, 2020, ActiveProspect experienced a security incident in which an unknown party gained access to our account data containing your personal information, as noted above. ActiveProspect learned of this potential security incident on November 20, 2020 and provided preliminary notice of the incident to Mead Johnson on December 2, 2020. Mead Johnson analyzed the account data and only became aware of the extent of the scope of the contents of the account data on February 23, 2021. This was the first time that ActiveProspect experienced a data breach. Since the incident, ActiveProspect has taken steps to remediate the security incident, including by instituting several administrative and technical safeguards, in order to minimize any inconvenience this incident may cause you. ActiveProspect hired a cybersecurity firm to track the affected account data online so that it can see if any data is shared or sold. None of the data has been identified on the dark web. ActiveProspect remains vigilant in continuing to monitor for the data online through the cybersecurity firm.

2. What Information Was Involved?

Your protected personal information that may have been compromised includes first and last name, and date of birth.

3. What Are We Doing?

ActiveProspect took the remediation steps described above as soon as it learned of the incident on November 20, 2020. Upon learning of the extent of the personal information compromised, Mead Johnson took further steps of providing you with this notice, and offering you complementary one-year membership of Experian's® IdentityWorks℠, which provides credit and identity monitoring. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by**: **June 30, 2021** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: https://www.experianidworks.com/credit
- Provide your **activation code**: **ABCDEFGHI**

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 833.671.0412 by June 30, 2021. Be prepared to provide engagement number B010269 as proof of eligibility for the identity restoration services by Experian.

4. What You Can Do?

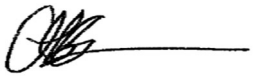
Mead Johnson does not believe that you need to do anything beyond the safeguards that it and ActiveProspect have already put in place. However, in case it may bring a sense of relief, please take advantage of the complimentary credit monitoring and identity theft services we are offering you. You may contact Experian's customer care team with any questions by calling our dedicated call center at 833.671.0412, from Monday through Friday, 6:00 am to 8:00 pm and Saturday and Sunday from 8:00 am to 5:00 pm Pacific Standard Time.

We encourage Mead Johnson consumers to remain vigilant. If helpful, there are additional details regarding your 12-month Experian IdentityWorks membership attached to this letter and further steps you can take to protect yourself contained in the supplement to this letter titled "**Additional Ways to Protect Your Identity: Important Identity Theft Information**."

5. For More Information

Mead Johnson remains committed to serving and protecting our consumers. If you have any questions regarding this incident, please contact Experian's customer care team at 833.671.0412.

Sincerely,



Annamarie Bermundo
Director, Consumer Engagement
Mead Johnson & Company, LLC

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only. *
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration agents are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™**: You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to $1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at 833.671.0412. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to you for one year from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

* Offline members will be eligible to call for additional reports quarterly after enrolling

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Additional Ways to Protect Your Identity: Important Identity Theft Information

Reviewing Your Accounts and Credit Reports

Be vigilant for the next 12 to 24 months and look out for any suspicious account activity. Regularly review your account statements, and periodically obtain your credit report from one or more of the three national credit reporting companies. Those companies are:

Equifax	**Experian**	**TransUnion**
1-800-525-6285	1-888-397-3742	1-800-680-7289
Equifax.com	Experian.com	Transunion.com

You can obtain your credit report from each of the companies listed above for free once every 12 months. Free reports are available online at www.annualcreditreport.com. You may also obtain a free report by calling toll free 1-877- 322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. If you do not have any free credit reports left, you can still purchase a copy of your credit report by contacting one or more of the credit reporting companies.

Placing a Fraud Alert

A fraud alert tells lenders that they should verify your identification before they extend credit in your name. Each of the three nationwide credit reporting companies can place a fraud alert on your credit report. If you wish to place a fraud alert, contact any one of the three credit reporting companies listed above. As soon as one company confirms your fraud alert, the others are notified to place fraud alerts as well.

Requesting a Security Freeze on Your Credit Report

A security freeze prohibits a credit reporting agency from releasing any information from your credit report without written authorization. Placing, lifting, or removing a security freeze is free of charge. To place a security freeze on your credit report, you must do so separately at each credit reporting company. The credit reporting companies do not notify each other about security freezes.

While a security freeze is in effect, it may delay, interfere with, or prevent the timely approval of any request you make for new credit, loans, mortgages, employment, housing or other services that require a credit check. If you want to allow a credit check for those or other purposes, you will have to lift the security freeze by contacting each credit reporting company. Each credit reporting agency will provide you a PIN number or a password when you place a security freeze. You will need that PIN or password to lift the freeze and should be careful to record it somewhere secure.

Suggestions if You Are a Victim of Identity Theft

If you find suspicious activity on your accounts or credit reports, or have other reason to believe your information is being misused, you should take the following steps:

File a Police Report. Get a copy of the report to submit to your creditors and others that may require proof of a crime.

Contact the U.S. Federal Trade Commission (FTC). The FTC provides useful information to identity theft victims and maintains a database of identity theft cases for use by law enforcement agencies. If you file an identity theft complaint with the FTC, your case will be added to that database. You can find more information and file a complaint online at www.identitytheft.gov. You can also file a complaint by calling the FTC's toll-free Identity Theft Hotline at 1-877-IDTHEFT (438-4338), or by mail at Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, N.W., Washington, D.C. 20580. You may also wish to obtain a copy of Identity Theft: A Recovery Plan, a guide from the FTC to help you guard against and deal with identity theft. It is available online at https://www.consumer.ftc.gov/articles/pdf-0009_identitytheft_a_recovery_plan.pdf.

Exercise Your Rights Under the Fair Credit Reporting Act (FCRA). You have certain legal rights under the FCRA. These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have credit reporting companies correct or delete inaccurate, incomplete, or unverifiable information. You can find more information about your rights under the FCRA online at https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf. The laws of your state may provide you with additional rights. Your state's attorney general or consumer protection department may be able to give you more information about your rights under state law.

Keep a record of your contacts. Start a file with copies of your credit reports, police reports, any correspondence, and copies of disputed bills. Keep a log of your conversations with creditors, law enforcement officials, credit reporting companies, and other relevant parties.